

6:21mj38

ATTACHMENT B

PROPERTY TO BE SEIZED

Evidence, instrumentalities, contraband, or fruits of violations of Title 21 United States Code, Section 841 (distribution and possession with intent to distribute controlled substances), Title 21 United States Code 846 (conspiracy), and Title 18, United States Code, Section 1956(h) (money laundering), (the TARGET OFFENSES), including the following:

a) Financial and business records, whether or not maintained electronically or by computer, including, but not limited to: books, records, receipts, notes, ledgers, journals, memoranda, address and/or telephone books, tapes, computer disks, computers relating to the transportation, ordering, purchase and distribution of controlled substances; United States currency, precious metals, jewelry and financial instruments, including but not limited to stocks and bonds;

b) Documents indicating travel in interstate and foreign commerce, to include airline tickets; notes and travel itineraries; airline schedules; bills; charge card receipts; hotel, motel, and car rental statements; correspondence with travel agencies and other travel-related businesses; airline, rent-a-car, and hotel frequent flier or user cards and statements; passports and visas; papers or documents of identity/nationality; telephone bills; photographs of foreign locations; and papers relating to domestic and international travel;

c) Books, records, receipts, bank statements and records, money drafts, letters of credit, money order and cashier's checks receipts, passbooks, bank checks, bank deposit tickets, safe deposit box keys, and memoranda and other items evidencing the

obtaining, secreting, transfer and/or concealment of assets and the obtaining, secreting, transfer, concealment and/or expenditure of money;

d) United States currency, precious metals, jewelry and financial instruments, including but not limited to stocks and bonds;

e) Photographs, in particular, photographs of co-conspirators, of assets and/or of controlled substances;

f) Indicia of occupancy, residence and/or ownership of the premises described above, including but not limited to utility and telephone bills, canceled envelopes, and keys;

g) Any and all firearms which may be used to facilitate transactions in controlled substances;

h) Mail matter (all classes), Priority Mail , Priority Mail Express, and International Mail parcels and packaging, DHL, FedEx, and UPS parcels and packaging, customs declarations and other records, and other correspondence which reflect names and addresses of suspected co-conspirators in the trafficking and mailing of drugs and cash proceeds; and

i) Any computer, computing device, laptops, tablet, smartphones, cellular telephones, external hard drives, computer hardware, software, related documentation, and electronic storage media, so that computer analysts can accurately retrieve the items authorized by this warrant in a laboratory or other controlled environment.

For any computer, laptops, cell phones, tablets, or storage medium, whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter,

“COMPUTER”):

- a) Any and all evidence related to the TARGET OFFENSES, including correspondence and/or communications,
- b) evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- c) evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- d) evidence of the lack of such malicious software;
- e) evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of COMPUTER access, use, and events relating to crime under investigation and to the COMPUTER user;
- f) evidence indicating the COMPUTER user’s state of mind as it relates to the TARGET OFFENSES;
- g) evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- h) evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- i) evidence of the times the COMPUTER was used;
- j) passwords, encryption keys, and other access devices that may be

necessary to access the COMPUTER;

k) documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

l) records of or information about Internet Protocol addresses used by the COMPUTER;

m) records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

n) contextual information from the COMPUTER necessary to understand the evidence described in this attachment.

In searching the COMPUTER, the federal agents may examine all of the data contained in the COMPUTER to view its precise contents and determine whether the COMPUTER and/or data falls within the items to be seized as set forth above. In addition, they may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth above.

For those COMPUTERS found within a search location where multiple individuals, in addition to the target of this investigation are located, federal agents will make reasonable efforts to ascertain whether the COMPUTER is used by or belongs to a target of the investigation to facilitate the commission of the TARGET OFFENSES. To the extent it becomes readily apparent that the COMPUTER was unlikely used in conjunction with or to facilitate in any way the commission of the TARGET OFFENSES, federal agents will not seize or search the COMPUTER beyond that which is necessary to ascertain the nature of its involvement in the

TARGET OFFENSES.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, gambling machines, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ITEMS TO BE SEIZED FROM ELECTRONIC STORAGE MEDIA

- A. Incoming and outgoing e-mails, chats, instant messages, texts messages, or any other types of communications, as well as call, text message, or other types of communication logs;
- B. Internet browser histories showing what internet sites were visited, for how long, and how often;
- C. Contact lists;
- D. Photo and video galleries;
- E. Navigation, mapping, and GPS files;
- F. For cellular telephones - telephone settings, including speed dial numbers and the telephone number for the subject telephone and related identifying information such as the ESN for the telephone;
- G. Evidence indicating who used the electronic device and when; and
- H. Any of the items set forth section I of this attachment that are capable of being stored electronically.